ESG Brief

RiskIQ Is Addressing Requirements for Outside-In Security

Date: October 2014 **Author:** Jon Oltsik, Senior Principal Analyst

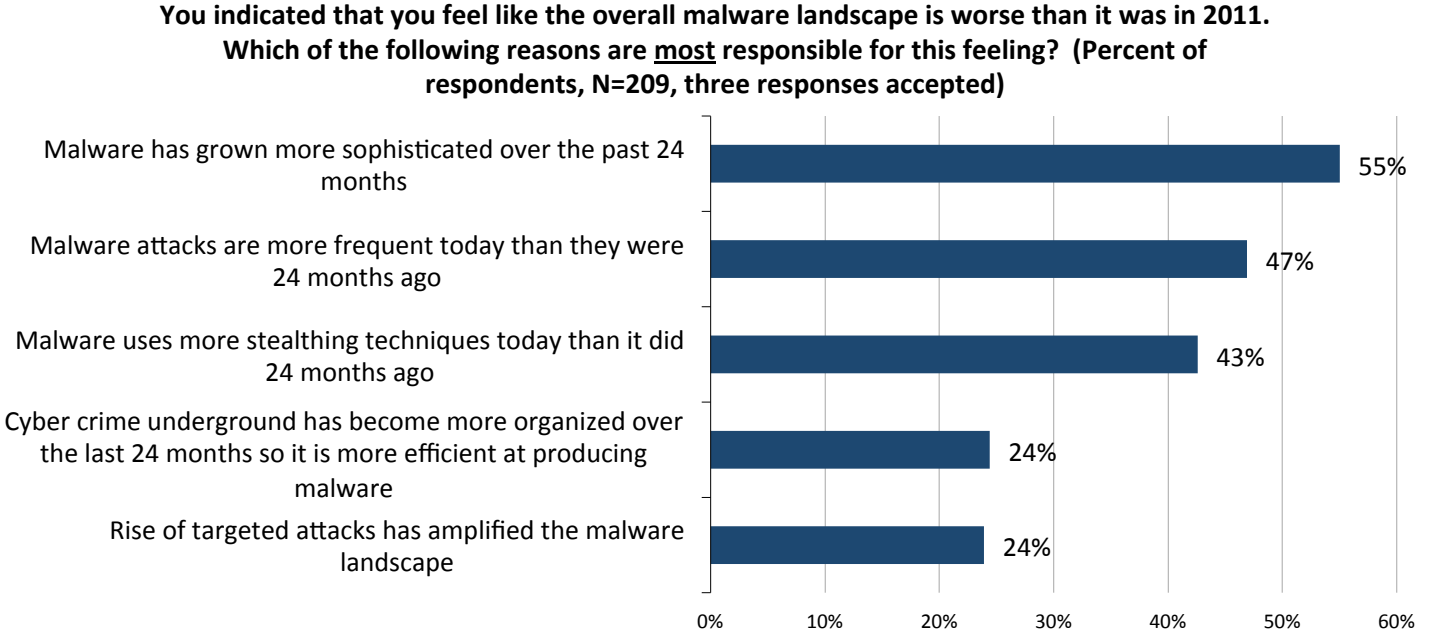
Abstract: *ESG research indicates that many security professionals feel like the malware threat landscape is getting worse. Why? Aside from targeted attacks conducted by cybercriminals and nation-states, hackers are getting more creative using ad networks, partner web sites, and mobile applications to attack organizations or steal personal data from customers. These threats emanate from outside the organization's network driving the need for outside-in security. Strong outside-in security requires continuous monitoring, specific threat intelligence, and a customer-centric view of risk. RiskIQ is one of the few companies focused in this area. According to several RiskIQ customers, the company is helping them address outside-in security risk management, improve threat detection, and accelerate remediation processes.*

Overview

According to a 2013 ESG research report, 30% of enterprise security professionals claimed that the malware landscape in 2013 was much worse than it was in 2011, while another 37% said that the malware landscape was somewhat worse in 2013 than in 2011. Why the malware skepticism? Of those security professionals who believe that the malware landscape had gotten worse, 55% said that malware had grown more sophisticated, 47% said that malware attacks had become more frequent, and 43% claimed that malware attacks were more stealthy than they were in the past (see Figure 1).[1]

These opinions aren't based solely on infosec paranoia. In fact, a number of security researchers believe that there will be somewhere between 25 to 30 million new malware threats in 2014 alone. Furthermore, many of these malware variants will be engineered with various obfuscation techniques in order to "fly under the radar" of security gateways, cloud security filters, and host-based security software.

Figure 1. Top Five Reasons Driving Increased Threat Perception



Source: Enterprise Strategy Group, 2014.

[1] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.

New Online Threats Abound

Recognizing the insidious malware threat, enterprise CISOs are bolstering their defenses. For example, ESG research indicates that, in 2013, 51% of large organizations indicated that they were planning to add new security technology controls to endpoint systems, 49% that they planned to collect and analyze more security data, and 44% that they planned to automate more security operations tasks.[2]

There is no doubt that these are all prudent and necessary steps. However, many enterprises are not addressing a variety of other emerging threat vectors. Today's enterprise IT environments should be viewed as a complex fabric of applications, users, B2B connections, and devices. While these interoperations can deliver business value, they also open new threat vectors that can impact an organization's employees, customers, or reputation. Enterprises face new cyber risks associated with:

- **Web sites.** Large organizations understand that they have to protect internal and external websites but what about the network of partner, distributor, and supplier sites that share applications or redirect users back and forth between corporate and third-party web properties? A "downstream" compromise could serve up malware to valued customers or be used as a staging site to steal valuable data.
- **Ad networks.** When working correctly, ad networks are designed to serve up targeted ads and thus attract highly-qualified customers. On the malevolent side however, ad networks have become a favorite hiding spot for black hats and crooks. In many cases, cybercriminals host "clean" ads, establish a footprint on an ad network, inject malware and spyware into a variety of different ads, and then piggyback on ad distribution networks to compromise end-user systems. Unfortunately, enterprises using these ad networks may find out that their ads have been compromised and are now being used for nefarious purposes. Malvertising is also used to deliver malware to specific targets using search terms, social networks, cookies, and other techniques.
- **Mobile applications.** Like phishing exploits of the past, cybercriminals are creating copycat mobile applications that look and feel like the real thing. These malicious mobile apps are posted on an assortment of certified and third-party app stores for distribution to unsuspecting users.

All of these threat vectors are particularly sinister as they compromise web-based real estate normally used to represent an organization to trusted online customers. In addition to these new risks, enterprises must also keep up with a morass of inaccurate and libelous content aimed at damaging an organization's reputation. Finding and removing this content efficiently could mean the difference between a destructive grapevine of rumors and a non-event. Organizations must be aware of these risks as they will always be held accountable for problems (whether they were responsible/culpable or not).

Large Organizations Need to Think About "Outside-In" Security

While organizations are investing in advanced security technologies, the new online threats described above have not been adequately addressed in many cases. What's more, large organizations can't possibly keep up with the scale, scope, volume, and constant change of these online threats using junior employees, search engines, and manual processes.

To address online threats efficiently and effectively, CISOs need to think in terms of "outside-in" security by assessing and addressing risks emanating from outside the corporate network that could cause harm to the organization, its customers, and other third-parties participating in the IT ecosystem (i.e., business partners, contractors, suppliers, etc.)

Effective outside-in security should include:

- **Continuous monitoring.** The first step in a comprehensive outside-in security model is identifying all websites, ad networks, mobile applications, and controversial content that may be downloaded, viewed, or used by customers. Of course, continuous monitoring is critical here as the list of potentially damaging web properties is in a constant state of change. Given this, CISOs should look for service providers with a

[2] Source: Ibid.

portfolio of web scanners, crawlers, and data analytics that can identify malicious sites and expedite remediation actions.

- **Malware distribution networks and threat actor intelligence.** To stay one step ahead of cybercriminals, organizations should make sure to correlate details about its web presence (i.e., all websites, ad networks, mobile app stores, etc.) with available threat intelligence (i.e., malicious IP addresses, URLs, C&C servers, malware distribution servers, etc.). Leading outside-in security tools will execute an immediate alert when threat intelligence intersects with any of the organization's customer-facing web assets.
- **Connection intelligence.** When it comes to cybercrime, it is foolish to judge any book by its cover. Web and mobile properties may look perfectly legitimate from the outside, but may contain malicious URLs and executables, or redirect users to exploit servers. Outside-in security tools must be able to understand the web of web connections and discover when a trustworthy activity spawns a malicious attack behind the scene.
- **Customer emulation tools.** Part of an outside-in security strategy is looking at security from a customer (or other third-party) perspective. In this regard, outside-in security tools should emulate user sessions that simulate customer interactions. Additionally, user emulation tools should be distributed in a variety of locations throughout the world in order to weed out targeted attacks, regional malware distribution sites, and sordid localized mobile apps. By emulating customer sessions, outside-in security tools should be able to see when an innocent interaction turns into a cyber-incident.

Introducing RiskIQ

While some progressive CISOs recognize the need for outside-in security, they often struggle to find the right technology solution to support these initiatives. For some, this means adopting an assortment of things like dynamic web application testing, malvertising protection, brand protection, web and social media scanning, and mobile application assessment services. Yes, this strategy may provide some protection, but managing multiple products or services can be costly and may greatly increase security operations overhead as the security team scrambles from console to console to assess and mitigate outside-in risk.

As an alternative to the complexities of multiple products and services, CISOs may want to look at RiskIQ, a San Francisco-based company. RiskIQ is actually one of the few one-stop-shops offering a number of outside-in security services. RiskIQ describes itself as follows:

RiskIQ was built with a purpose in mind: obtaining visibility over the endless landscape that is the great unknown–the Web. We view ourselves as an organization that is personally taking on the task of ensuring that the web and mobile landscapes go from being uncharted blobs of unknown risk, to carefully charted maps that ensure complete visibility.

RiskIQ provides outside-in security services in four areas:

1. **Mobile application security.** RiskIQ automates the discovery of mobile apps and partner apps. When a rogue app is discovered, RiskIQ initiates a virtual user session to interrogate the app and uncover the interaction real users are experiencing with it. The RiskIQ technology then grabs the API, analyzes the app for third-party content, over-reaching permissions, and nefarious referring URLs. When a copycat or hacked app is detected, RiskIQ notifies its customers and takes it down.
2. **Malvertising and malware prevention.** RiskIQ scans, analyzes, and tracks advertisements through the ad network supply chain to detect, classify, and report on suspicious activity and also identify confirmed malvertisements. Armed with this intelligence, security teams can prioritize and accelerate remediation activities.
3. **Brand and trademark protection.** RiskIQ monitors the web (i.e., advertisements, blogs, mobile apps, and websites) for trademark misuse and abuse. It also categorizes these incidents based on their potential damage.
4. **Website security.** RiskIQ scans the open web, to identify an organization's ownership of web assets and their respective dependencies. Once these assets are discovered, RiskIQ initiates a virtual user session that mimicks a real internet user, executes a full DOM and packet capture, and then enriches that data against its global threat

intelligence database. This can provide RiskIQ customers with a complete view of what an asset is doing and how it might be interacting with known bad actor domains. Once benign assets are under management, RiskIQ will then continuously monitor them for changes, suspicious behavior, and overt threats.

RiskIQ and its Customer Value

To get a better understanding of outside-in security, ESG recently spoke to three RiskIQ customers in the financial services industry.

Security professionals working at financial services organizations clearly believe that the outside-in security threat is real and growing:

"I've got to admit that I was a 'doubting Thomas' at first so I was amazed when we started to find all kinds of rogue websites and mobile applications claiming they were ours. I went from being a skeptic to being really scared." (Security manager, global banking company)

"I knew about malvertising but had no idea how bad the situation is. I know now!" (Threat analyst, global financial services company)

"We didn't find too many copycat mobile applications at first but I have to say that the numbers keep growing—especially in Asia." (Security professional, US-based bank)

Each respondent spoke about the special needs and challenges of outside-in security and why they chose to work with RiskIQ:

"My first instinct was to have a few junior employees do Google searches and identify any suspicious websites using our name. It didn't take long for me to realize that this type of manual process couldn't scale. That's when we understood why we needed an automated service like RiskIQ." (Security manager, global banking company)

"This isn't just about text, it's about discovering images and graphics down to the pixel level to know if it's ours or not. RiskIQ can do this, my staff can't." (Threat analyst, global financial services company)

"We have multiple groups involved, including the application monitoring group on the mobile side and the threat intelligence group within security. Everyone has slightly different needs but it made sense to try and work together. RiskIQ helps us accomplish this." (Security professional, US-based bank)

Finally, all three security professionals interviewed said that RiskIQ has delivered value to their organizations in two primary areas: Detecting rogue web and mobile assets, and accelerating remediation processes.

"RiskIQ captures a lot of data. We've learned how to tune our parameters so we can get accurate and detailed information quickly. I feel like we are miles ahead of where we were last year in terms of finding copycat websites and taking them offline." (Security manager, global banking company)

"As we learn how big this problem is, we see more and more value out of RiskIQ." (Threat analyst, global financial services company)

"We started with the mobile use case and expanded from there. We also started talking to other groups within the bank to educate them about RiskIQ and see if they can use it too. Many of these discussions are headed in a positive direction." (Security professional, US-based bank)

The Bigger Truth

Most security professionals recognize that cloud computing, mobile applications, and multi-site web applications can increase IT risk. Unfortunately, few organizations understand the intricacies of these risks or what it will take to address them. Some try to get by with manual processes for risk assessment while others use an army of tools and services. Each of these strategies is severely flawed and cannot keep up with an environment highlighted by constant change, massive scale, and increasingly stealthy threats.

In truth, outside-in security introduces new risks, demanding new strategies and technologies for risk mitigation. CISOs need a combination of continuous monitoring, malware distribution and threat actor intelligence, connection intelligence, and customer emulation tools to detect and mitigate threats in real-time. RiskIQ has built a series of outside-in services for this very purpose. Based upon several customer issues, RiskIQ seems to be meeting user requirements and delivering unique outside-in security value.